

BAB I PENDAHULUAN

Bab satu menjelaskan mengenai latar belakang, perumusan masalah, tujuan penelitian, tujuan dan manfaat penelitian, batasan, dan sistematika penulisan. Latar belakang berfokus pada penjelasan dari permasalahan yang terjadi pada objek yang diambil untuk penelitian. Bab ini juga membahas tentang perumusan masalah yang berisi tentang masalah akan dibahas lebih rinci pada penelitian ini.

1.1 Latar Belakang

Dalam tugas akhir ini mengambil studi kasus PT. Akses Kualitas Unggul (PT. AKU) sebagai perusahaan yang bergerak di bidang jasa konstruksi sebagai mitra dari PT. Telkom Indonesia. PT. AKU berusaha memberikan kinerja terbaik dalam berbagai *project* pekerjaan yang diberikan oleh anak perusahaan PT. Telkom Indonesia yakni PT. Telkom Akses.

Dalam mengatur data dari pegawai PT. AKU masih menggunakan pendataan manual dalam *excel* pada penyimpanan lokal di laptop kantor. Oleh karena itu, penelitian ini akan membantu untuk membuat sistem pendataan pegawai sederhana yang berisikan data pegawai dari PT. AKU yang berupa aplikasi berbasis web dan akan mengimplementasikan penerapan metode algoritma RC4 pada *database* website PT. AKU. Waktu proses enkripsi algoritma RC4 pada *database* juga menjadi bagian dalam penelitian.

Kriptografi berasal dari Bahasa Yunani: “cryptós” artinya rahasia, sedangkan “gráphein” artinya tulisan. Sehingga, secara morfologi kriptografi dapat diartikan sebagai tulisan rahasia[1]. Definisi yang dipakai dalam tulisan ini: Kriptografi merupakan ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentifikasi[2]. Oleh karena itu, topik kriptografi dipilih dalam penyusunan skripsi untuk membantu mengamankan data sensitif pegawai PT. AKU.



Penelitian ini menggunakan metode algoritma RC4. Algoritma enkripsi RC4 (Rives Code 4) merupakan algoritma yang menggunakan kunci simetris berupa *stream cipher* yang dibuat oleh RSA Data Security Inc (RSADSI). Algoritma ini ditemukan oleh Ronald Rivest pada tahun 1987 dan telah menjadi simbol keamanan RSA (nama dari tiga penemunya: Rivest Shamir Adleman). RC4 menggunakan panjang kunci dari 1 hingga 256 byte yang digunakan untuk menginisialisasi tabel 256 byte. Tabel ini digunakan untuk nomor pseudo-random generasi berikutnya yang menggunakan XOR dan plaintext untuk menghasilkan ciphertext. Setiap elemen dalam tabel dipertukarkan setidaknya sekali.[1]

RC4 adalah jenis stream cipher [3] yang memproses unit atau input data satu per satu. Dengan cara ini pengguna dapat melakukan enkripsi atau dekripsi panjang variabel. Algoritma tidak perlu menunggu sejumlah data input tertentu sebelum memproses atau menambahkan byte tambahan untuk dikodekan. Metode enkripsi RC4 sangat cepat, sekitar sepuluh kali lebih cepat dari DES.[1]

Menurut penelitian yang dilakukan oleh A. Andrico and M. J. S. Syafrullah pada tahun 2018 yang berjudul "Aplikasi Enkripsi Database Menggunakan Algoritma Rc4 Berbasis Desktop" maka peneliti dapat mengambil benang merah dan kesimpulan yaitu algoritma kriptografi RC4 berhasil diimplementasikan dalam melindungi nilai siswa pada database sekolah SMK KARTIKA X2 menggunakan algoritma kriptografi RC4 berbasis desktop untuk mengamankan data sehingga tidak dapat disalahgunakan oleh pihak yang tidak bertanggungjawab.[3]

Keunggulan dari metode algoritma kriptografi RC4 ini adalah data yang telah terenkripsi tidak dapat/sangat sulit untuk membukanya bila tidak memiliki kunci. Hasil enkripsi data tidak akan mengalami perubahan dan dapat digunakan kembali oleh admin dengan mendekripsi data tersebut sehingga menjadi *plaintext* seperti semula. Namun metode ini memiliki kekurangan yaitu semakin panjang *plaintext* yang diisikan maka semakin panjang *len* enkripsi data yang dilakukan oleh *database* dan membutuhkan waktu enkripsi yang semakin lama.[3]



Dalam penelitian yang dilakukan oleh G. Ammary and S. J. S. Mulyati pada tahun 2018 dengan judul "Aplikasi Kriptografi Untuk Keamanan Database Dengan Metode RC4 dan ELGAMAL Berbasis Web Pada JXL Design Co." Penggunaan metode algoritma kriptografi RC4 dalam mengamankan data sensitif pegawai lebih cepat dari metode DES dan dapat diaplikasikan pada aplikasi web perusahaan menggunakan bahasa pemrograman Java atau PHP pada *database* MySQL.[4]

Oleh karena itu, pada tugas akhir ini akan mengimplementasikan algoritma enkripsi RC4 pada sistem website yang dilakukan pada sisi server. pada tugas akhir ini juga akan menganalisa kualitas algoritma enkripsi RC4 dengan metode Avalanche Effect serta melakukan percobaan penyerangan Brute Force algoritma RC4 untuk mengukur estimasi waktu yang dibutuhkan untuk memecahkan seluruh kemungkinan kunci. [3, 5].

1.2 Perumusan Masalah

Berdasarkan uraian latar belakang diatas maka dapat dipaparkan rumusan masalah sebagai berikut :

1.2.1 Permasalahan

Belum adanya sistem untuk mendata pegawai di perusahaan karena proses pendataan pegawai masih dilakukan secara manual. Banyaknya data sensitif dari pegawai yang merupakan arsip perusahaan yang hanya terdata dalam bentuk Excel dan disimpan dalam penyimpanan lokal admin pegawai, sehingga data sensitif mudah terekspose dan dapat digunakan oleh pihak yang tidak bertanggung jawab. Penyimpanan data pada *harddisk* lokal juga kurang efektif karena masih menggunakan input *manual* pada aplikasi Microsoft Excel. Penyimpanan dalam *harddisk* lokal tersebut dinilai peneliti memiliki banyak kekurangan, sebagai contoh apabila laptop admin perusahaan mengalami kerusakan maka tidak dapat memperbaharui, menambah, menghapus data untuk sementara waktu. Contoh lain adalah jika admin perusahaan *resign* dari perusahaan, ada kemungkinan data pribadi pegawai masih dapat diakses oleh admin dan



memiliki kemungkinan untuk disalahgunakan.

1.2.2 Usulan Solusi

Berdasarkan permasalahan yang ditemukan oleh penulis, maka penulis berinisiatif untuk membuat sistem pendataan pegawai berbasis web untuk penyimpanan data pribadi pegawai perusahaan berbasis web dan menerapkan enkripsi simetris menggunakan metode algoritma RC4 untuk memudahkan admin perusahaan dalam melakukan pendataan dan mengamankan data pegawai.



1.2.3 Pertanyaan Penelitian

1. Seberapa banyak perubahan bit yang terjadi pada ciphertext hasil enkripsi algoritma enkripsi RC4?
2. Berapa waktu yang dibutuhkan untuk melakukan serangan Brute Force pada algoritma enkripsi RC4?

1.3 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari penelitian ini adalah:

1.3.1 Tujuan Penelitian

Penelitian ini bertujuan untuk mengimplementasikan metode algoritma enkripsi RC4 (*Rivest Cipher 4*) dalam melakukan pendataan pegawai berbasis website. Peneliti berusaha untuk menjawab pertanyaan penelitian tentang bagaimana mengukur kualitas enkripsi, dengan mengukur kualitas enkripsi melalui metode pengujian *Avalanche Effect*. Tujuan penelitian ini juga berusaha mencari kesimpulan apakah enkripsi menggunakan metode algoritma RC4 layak digunakan atau tidak. Peneliti juga akan menguji dengan memberikan gangguan dengan menggunakan *bruteforce* algoritma enkripsi RC4 untuk menguji waktu yang dibutuhkan untuk memecahkan *ciphertext*

1.3.2 Manfaat Penelitian

Manfaat dari penelitian ini adalah untuk membantu perusahaan dalam mengamankan data pegawai dengan menerapkan algoritma enkripsi RC4 (*Rivest Cipher 4*) dengan *form input* berbasis website sebagai sistem pengganti pada pendataan manual perusahaan. Manfaat berikutnya adalah mendapatkan data dari kualitas enkripsi RC4 dan dapat dibandingkan dengan metode enkripsi lain dalam penelitian lain.

1.4 Batasan-batasan

Batasan masalah diperlukan guna penelitian tetap terarah dan fokus pada hal yang diteliti, batasan tersebut diantaranya :

1. Data yang digunakan dalam penelitian ini adalah data pegawai PT AKSES KWALITAS UNGGUL tahun 2022



2. Implementasi RC4 berbasis website dengan form input sederhana
3. Menggunakan MySQL sebagai database
4. *Brute Force* algoritma enkripsi RC4
5. Pengujian *Avalanche Effect* membandingkan dengan panjang kunci yang berbeda
6. Pengujian *bruteforce* algoritma enkripsi RC4 menguji lama waktu pemecahan *ciphertext* RC4

1.5 Sistematika Penulisan

Sistematika penulisan akan menguraikan menjadi beberapa bab yang secara garis besar adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi tentang latar belakang, perumusan masalah, tujuan dan manfaat pada penelitian, batasan-batasan, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini dijelaskan mengenai teori-teori yang mendukung dan membahas mengenai penelitian terkait.

BAB III METODOLOGI PENELITIAN

Pada bab ini menguraikan tentang gambaran umum metode algoritma RC4, analisis kerja sistem, analisis kebutuhan sistem, perancangan sistem, simulasi perhitungan RC4 dan skenario pengujian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini akan memaparkan hasil dan pembahasan meliputi pembuatan website (*User Interface*, dan implementasi algoritma enkripsi RC4 pada sisi server), hasil pengujian *Avalanche Effect* dan pengujian *Brute Force* algoritma RC4.

BAB V PENUTUP

Pada bab ini akan memaparkan kesimpulan dari hasil pengujian dan saran terkait penelitian ini

